

Meeting notes for May 10, 2004 I++ DME implementer's conference call

Meeting secretary: John Horst
The National Institute of Standards and Technology (NIST)
Telephone: 301.975.3430
Email: john.horst@nist.gov

May 10, 2004

Name	Organization	Present
Ray Admire	Lockheed Martin	
Manfred Becker	Zeiss	
Perluigi Borgogno	Wilcox Associates	✓
Joe Falco	NIST	
Swen Haubold	Mitutoyo	
John Horst	NIST	✓
René Keller	Metromec	
Tom Kramer	NIST	✓
Chuck Leckenby	Tecnomatix	
Mike Martini	General Electric Transportation	
Günter Moritz	Messtechnik Wetzlar	
Michel Penlae	Wilcox Associates	✓
Chiratana Pot	Tecnomatix	✓
Walter Punegam	Zeiss	
Josef Resch	Zeiss	✓
Bill Rippey	NIST	✓
John Rosser	Renishaw	
Ken Sheehan	Entelegence	
Dave Smith	LK	✓
Rob Stewart	Daimler-Chrysler	✓
Keith Stouffer	NIST	
Tim Taylor	General Electric Transportation	
Mark Vinson	Boeing	
Bob Waite	Daimler-Chrysler	
Betsy Weddendorf	General Electric Transportation	
Martin Wimmer	Zeiss	✓

1 Discussion of topics relating to the planned IMTS demo (of I++ DME interoperability)

John sought further input from the group on how we are to accomplish the planned IMTS demo of I++ DME interoperability. He expressed the opinion that NIST needs to have copies of I++ DME-compliant client applications in order to make sure that we can accomplish a semi-automated execution of the planned scenario for the demo (see April 5, 2004 meeting notes). Martin Wimmer suggested we speak with Zeiss people at Brighton, Michigan (USA) about software. Michel said all that is needed to run PCDMIS in I++ DME mode is to use the correct .dll (which he can provide) and get the correct authorization in the key from Ken Woodbine. Michel also reiterated that PCDMIS can be started and stopped from a computer remotely located on a LAN via a batch file. Dave Smith mentioned LK's plans to start on a client implementation later this month and that, like PCDMIS, can run their client remotely

from a batch file.

Josef questioned whether it might be better to ensure the correct execution of client and server from the vendor geographic locations remotely as we have been planning before we work on execution at NIST under the IMTS demo scenario. John said that we want to do both at the same time, if possible.

Chiratana asked for CAD files with tolerances for the planned demo artifact. NIST has these files, which they received from DCX, and will distribute them at the appropriate time (when all other files are ready).

Rob suggested that we look at a more expanded set of CMM tasks for the IMTS demo including select and calibrate probe, alignment, and inspection (of only one or a few features). Josef suggested that such a sequence of tasks would take a long time during the demo.

John mentioned that we need to have a more complex set of features measured in order to demonstrate DML, which is also planned.

Michel pointed out that DML in the demo complicates things, since we need DML compliance and I++ DME compliance in the same application software. John said he would work on this.

2 Discussion of successes in (and barriers to) client \longleftrightarrow server connections

Bill introduced information about VPN connections with NIST, that was emailed to the group last week. He asked the group whether anyone is opposed in principle to this general method of connection. Here were the options proposed by NIST:

Option 1: Here is a minimum configuration of what we would need to setup a VPN link between NIST and a collaborator's VPN endpoint: IKE Security Association (SA) using pre-shared secret (we will exchange this either in person or using another encrypted means such as PGP encrypted email) Exchange mode: Main Phase 1 Diffie-Hellman (DH): Group 2 key exchange SA lifetime: 28,800 Phase 1 Encryption/Authentication: 3DES/SHA1 Phase 2 Encryption/Authentication: ESP 3DES HMAC SHA1 (Encapsulation Security Protocol/Keyed-Hash Message Authentication Code)

Option 2: If there are only a few people/computers at the collaborator's site, a better option would be for NIST to send the collaborator a preconfigured VPN client software package (NIST will supply this). The collaborator(s) would then install the software on their PC, with the settings already configured to talk to our VPN. Each collaborator would also receive a NIST authenticator card. The collaborator would have to authenticate to the NIST firewall using a one-time password before setting up the VPN link.

Option 3: Modem to modem connections. Currently not preferred by the NIST IT staff.

Option 2 seemed most agreeable to all and, since NIST prefers it as well, that option will be the preferred option for client to server communications with the NIST testbed.

3 New and outstanding action items

- NIST will obtain or generate a DMIS program for inspecting the DCX part and distribute this (along with CAD) to the group for comment and implementation in their client software.
- NIST will work to obtain commitments from I++ DME compliant CMM vendors and I++ DME and DML compliant software vendors to participate in the IMTS demonstration.

Our next meeting is planned for May 24, 2004. Talk with you then!